Also available on
SCIENCE DIRECT®
www.sciencedirect.com

ELSEVIER

European Journal of Combinatorics 24 (2003) 1089–1096

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Fonctions de partitions à parité périodique

Houda Lahouar

Département de Mathématique, Faculté des Sciences de Monastir, 5000 Monastir, Tunisie

Reçu le 19 décembre 2002; accepté le 29 avril 2003

Abstract

Let $\mathbb{N}$ be the set of positive integers and $\mathcal{A}$ a subset of $\mathbb{N}$. For $n \in \mathbb{N}$, let $p(\mathcal{A}, n)$ denote the number of partitions of n with parts in $\mathcal{A}$. In the paper J. Number Theory 73 (1998) 292, Nicolas et al. proved that, given any $N \in \mathbb{N}$ and $\mathcal{B} \subset \{1, 2, \ldots, N\}$, there is a unique set $\mathcal{A} = \mathcal{A}_0(B, N)$, such that $p(\mathcal{A}, n)$ is even for $n > N$. Soon after, Ben Saïd and Nicolas (Acta Arith. 106 (2003) 183) considered $\sigma(\mathcal{A}, n) = \sum_{d|n, d\in\mathcal{A}} d$, and proved that for all $k \geq 0$, the sequence $(\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1})_{n\geq 1}$ is periodic on n. In this paper, we generalise the above works for any formal power series f in $\mathbb{F}_2[z]$ with $f(0) = 1$, by constructing a set $\mathcal{A}$ such that the generating function $f_{\mathcal{A}}$ of $\mathcal{A}$ is congruent to f modulo 2, and by showing that if $f = P/Q$, where P and Q are in $\mathbb{F}_2[z]$ with $P(0) = Q(0) = 1$, then for all $k \geq 0$ the sequence $(\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1})_{n\geq 1}$ is periodic on n.

1. Introduction

On note par $\mathbb{N}$ l'ensemble des entiers strictement positifs, $\mathcal{A}$ un sous-ensemble de $\mathbb{N}$ et par $A(x)$ sa fonction de compte définie comme suit

$$A(x) = \mathrm{Card}\{a : a \leq x, a \in \mathcal{A}\}. \tag{1}$$

Si $\mathcal{A} = \{n_1, n_2, \ldots\} \subset \mathbb{N}$ (avec $n_1 < n_2 < \cdots$), alors $p(\mathcal{A}, n)$ désigne le nombre de partitions de n dont les parts appartiennent $\mathcal{A}$, c'est le nombre de solutions de l'équation

$$n_1 x_1 + n_2 x_2 + \cdots = n,$$

où $x_1, x_2, \ldots$ désignent des entiers positifs ou nuls. Par convention, on pose $p(\mathcal{A}, 0) = 1$ et $p(\mathcal{A}, n) = 0$ pour $n < 0$. La fonction génératrice associée à l'ensemble $\mathcal{A}$ s'écrit

$$F_{\mathcal{A}}(z) = \sum_{n=0}^{\infty} p(\mathcal{A}, n) z^n = \prod_{a\in\mathcal{A}} \frac{1}{1 - z^a}. \tag{2}$$

E-mail address: houda_lahouar@yahoo.fr (H. Lahouar).

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/S0195-6698(03)00115-X

Par la suite, on notera par $\chi(\mathcal{A}, n)$ la fonction caractéristique de $\mathcal{A}$

$$\chi(\mathcal{A}, n) = \begin{cases} 1 & \text{si } n \in \mathcal{A} \\ 0 & \text{si } n \notin \mathcal{A}. \end{cases} \tag{3}$$

Pour $n \geq 1$, on désigne par

$$\sigma(\mathcal{A}, n) = \sum_{d|n} \chi(\mathcal{A}, d)d = \sum_{d|n, d\in\mathcal{A}} d. \tag{4}$$

Dans les articles [6] et [7], on montre que si $\mathcal{B} = \{b_1, \ldots, b_k\} \neq \emptyset$ (avec $1 \leq b_1 < \cdots < b_k$) est un sous-ensemble fini de $\mathbb{N}$, $N \geq \max B$, alors il existe un ensemble unique $\mathcal{A} \subset \mathbb{N}$, tel que

$$\mathcal{A} \cap \{1, 2, \ldots, N\} = \mathcal{B}, \tag{5}$$

et

$$p(\mathcal{A}, n) \equiv 0 \pmod 2 \qquad \text{pour tout } n \in \mathbb{N}, n > N. \tag{6}$$

On note cet ensemble par $\mathcal{A} = \mathcal{A}_0(B, N)$. La construction de $\mathcal{A}_0(B, N)$ se fait par récurrence (cf. [6, 7]): si, pour $n \geq 1$, on pose

$$\mathcal{A}_n = \mathcal{A} \cap \{1, 2, \ldots, n\}, \tag{7}$$

alors

$$\mathcal{A}_N = \mathcal{A} \cap \{1, 2 \ldots, N\} = \mathcal{B}. \tag{8}$$

Si $n \geq N + 1$ et $\mathcal{A}_{n-1}$ défini par (7), alors $p(\mathcal{A}, m)$ est pair pour tout $N + 1 \leq m \leq n - 1$. On a

$$n \in \mathcal{A}, \qquad n \geq N + 1 \Longleftrightarrow p(\mathcal{A}_{n-1}, n) \text{ est impair.} \tag{9}$$

D'après cette construction, on a pour tout $n \geq N + 1$

$$\begin{aligned} &\text{si } n \in \mathcal{A}, && p(\mathcal{A}, n) = 1 + p(\mathcal{A}_{n-1}, n), \\ &\text{si } n \notin \mathcal{A}, && p(\mathcal{A}, n) = p(\mathcal{A}_{n-1}, n). \end{aligned}$$

Dans [7], on définit le polynôme caractéristique $P \in \mathbb{F}_2[z]$ associé à $\mathcal{A} = \mathcal{A}_0(B, N)$ par

$$P(z) = \sum_{0\leq n\leq J} \varepsilon_n z^n, \tag{10}$$

où J désigne le plus grand entier tel que $p(\mathcal{A}, J)$ soit impair et ε_n vérifie la relation

$$p(\mathcal{A}, n) \equiv \varepsilon_n \pmod 2, \qquad \varepsilon_n \in \{0, 1\}, \qquad 0 \leq n \leq J. \tag{11}$$

Soient $A(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathbb{Z}[[z]]$ et $B(z) = \sum_{n=0}^{\infty} b_n z^n \in \mathbb{Z}[[z]]$ deux séries formelles à coefficients entiers. Si M est un nombre entier positif, on dit que $A \equiv B \pmod M$ si, pour tout $n \geq 0$, on a $a_n \equiv b_n \pmod M$. Par (2), (6), (10) et (11), le polynôme caractéristique P vérifie la relation suivante

$$F_{\mathcal{A}}(z) \equiv P(z) \pmod 2. \tag{12}$$

Soit maintenant $f(z) = \sum_{n=0}^{\infty} \varepsilon_n z^n$, avec $\varepsilon_n \in \{0, 1\}$ et $\varepsilon_0 = 1$. Par un procédé voisin de celui utilisé dans la construction de $\mathcal{A}_0(\mathcal{B}, N)$, on peut montrer qu'il existe un ensemble unique $\mathcal{A}(f) \subset \mathbb{N}$ tel que

$$F_{\mathcal{A}(f)}(z) = \prod_{a \in \mathcal{A}(f)} \frac{1}{1 - z^a} = \sum_{n=0}^{\infty} p(\mathcal{A}(f), n) z^n \equiv f(z) \pmod 2 \tag{13}$$

autrement dit

$$p(\mathcal{A}(f), n) \equiv \varepsilon_n \pmod 2, \qquad n = 1, 2, 3, \ldots. \tag{14}$$

En effet, pour $n = 1$,

$$p(\mathcal{A}(f), 1) = \begin{cases} 1 & \text{si } 1 \in \mathcal{A}(f) \\ 0 & \text{si } 1 \notin \mathcal{A}(f) \end{cases}$$

et donc, par (14),

$$1 \in \mathcal{A}(f) \Longleftrightarrow \varepsilon_1 = 1. \tag{15}$$

Ensuite, supposant les éléments de $\mathcal{A}(f)$ connus jusqu'à $n - 1$, on pose $(\mathcal{A}(f))_{n-1} = \mathcal{A}(f) \cap \{1, 2, \ldots, n - 1\}$ et (9) devient, par (14)

$$n \in \mathcal{A}(f) \Longleftrightarrow p((\mathcal{A}(f))_{n-1}, n) \equiv 1 + \varepsilon_n \pmod 2. \tag{16}$$

Soit P un polynôme de degré J. En considérant P comme une série formelle dont les coefficients d'indice supérieurs à J sont nuls, on peut définir $\mathcal{A}(P)$ par (15) et (16). Les rapports entre $\mathcal{A}(P)$ et $\mathcal{A}_0(\mathcal{B}, N)$ défini par (5) et (6) sont les suivants: étant donné $\mathcal{B} \subset \{1, 2, \ldots, N\}$, on construit le polynôme caractéristique par (10) et (11); par (11) et (16) (pour les $n \le N$) et par (9) et (16) (pour les $n > N$), on voit que $\mathcal{A}(P) = \mathcal{A}_0(\mathcal{B}, N)$. Réciproquement, si on se donne un polynôme $P \in \mathbb{F}_2[X]$ de degré J, alors, pour tout $N > J$, en posant $\mathcal{B}_N = \mathcal{A}(P) \cap \{1, 2, \ldots, N\}$, on a $\mathcal{A}_0(\mathcal{B}_N, N) = \mathcal{A}(P)$.

Dans [1] (cf. aussi [3]), la propriété suivante a été donnée pour $\mathcal{A}(P)$ lorsque P est un polynôme: pour tout $k \ge 0$, la suite $(\sigma(\mathcal{A}(P), 2^k n) \bmod 2^{k+1})_{n \ge 1}$ est périodique de période T_k, autrement dit

$$\sigma(\mathcal{A}(P), 2^k(n + T_k)) \equiv \sigma(\mathcal{A}(P), 2^k n) \pmod{2^{k+1}}. \tag{17}$$

La période T_k a les propriétés suivantes: pour tout $k \ge 0$,

$$T_k \text{ est impair}, \qquad T_k \text{ divise } T_{k+1}, \qquad \text{pour } k \ge k_0, \qquad T_k = T \text{ fixé}. \tag{18}$$

En appliquant la formule d'inversion de Möbius à (4), les propriétés (17) et (18) permettent de calculer la fonction $\chi(\mathcal{A}, n)$ définie en (3) et ainsi, de déterminer les éléments de l'ensemble $\mathcal{A}(P)$ (cf. [2, 8] et [4]). Dans cet article, nous nous proposons d'étudier l'ensemble $\mathcal{A}(P/Q)$ où $P, Q \in \mathbb{F}_2[z]$ sont deux polynômes tels que

$$P(0) = Q(0) = 1, \qquad (P, Q) = 1. \tag{19}$$

La division de P par Q dans $\mathbb{F}_2[z]$ donne

$$f(z) = \frac{P(z)}{Q(z)} = \sum_{i=0}^{\infty} \varepsilon_i z^i, \qquad \varepsilon_i \in \{0, 1\}.$$

On construit l'ensemble $\mathcal{A}(f) = \mathcal{A}(P/Q)$ par (15) et (16). La fonction génératrice $F_{\mathcal{A}(P/Q)}$ associée à $\mathcal{A}(P/Q)$ vérifie, par (13), la relation

$$F_{\mathcal{A}(P/Q)}(z) = \sum_{n=0}^{\infty} p(\mathcal{A}(P/Q), n) z^n \equiv \frac{P(z)}{Q(z)} \pmod 2. \tag{20}$$

Dans la Section 2 (Théorème 2.1), on montre que pour tout $P, Q \in \mathbb{F}_2[z]$ satisfaisant (19), il existe un polynôme $U \in \mathbb{F}_2[z], U(0) = 1$ tel que les ensembles $\mathcal{A}(P/Q)$ et $\mathcal{A}(U)$ diffèrent par un ensemble d'entiers de la forme $2^h L, h \in \mathbb{N}$. Dans la Section 3 (Théorème 3.1), on montre que pour tout k entier positif, la suite $(\sigma(\mathcal{A}(P/Q), 2^k n) \bmod 2^{k+1})_{n\geq 1}$ est périodique. Si on note par q_k la plus petite des périodes, on a q_k divise q_{k+1} et pour tout $k \geq k_0$, on a $q_k = \mathrm{ppcm}(T_k, L) = q$, où T_k désigne la plus petite des périodes de la suite $(\sigma(\mathcal{A}(U), 2^k n) \bmod 2^{k+1})_{n\geq 1}$.

2. Construction de $\mathcal{A}(P/Q)$ à partir de $\mathcal{A}(U)$

On appelle ordre du polynôme Q dans $\mathbb{F}_2[z]$ le plus petit entier $L > 0$ tel que $Q(z)$ divise $1 + z^L$ dans $\mathbb{F}_2[z]$ (cf. [9], Chapter 3).

Théorème 2.1. *Soient $P, Q \in \mathbb{F}_2[z]$ satisfaisant (19), et $\mathcal{A}(P/Q)$ l'ensemble défini par (20). Si on note par L l'ordre de Q dans $\mathbb{F}_2[z]$, alors il existe un polynôme unique $U \in \mathbb{F}_2[z], U(0) = 1$, tel que, en définissant $\mathcal{A}(U)$ par (15) et (16)*

- *1ème cas: s'il existe un entier $h \geq 0$ tel que $\{L, 2L \ldots, 2^{h-1}L\} \subset \mathcal{A}(U)$ et $2^h L \notin \mathcal{A}(U)$, alors on a*

$$\mathcal{A}(P/Q) = \mathcal{A}(U) \backslash \{L, 2L, \ldots, 2^{h-1}L\} \cup \{2^h L\}, \tag{21}$$

l'ensemble $\{L, 2L, \ldots, 2^{h-1}L\}$ étant vide lorsque $h = 0$.

- *2ème cas: si, pour tout $h \geq 0$, $2^h L \in \mathcal{A}(U)$ alors*

$$\mathcal{A}(P/Q) = \mathcal{A}(U) \backslash \{\cup_{i=0}^{\infty} 2^i L\}. \tag{22}$$

Démonstration. D'après la définition de l'ordre d'un polynôme, il existe $W \in \mathbb{F}_2[z]$ tel que

$$1 - z^L = Q(z) W(z). \tag{23}$$

D'après (23) et (20), la fonction génératrice associée $\mathcal{A}(P/Q)$ s'écrit

$$F_{\mathcal{A}(P/Q)}(z) \equiv \frac{P(z)}{Q(z)} \equiv \frac{U(z)}{1 - z^L} \pmod 2, \tag{24}$$

avec $U(z) = P(z) W(z) \in \mathbb{F}_2[z]$.

- 1*ème* cas. Si $L \notin \mathcal{A}(U)$, on a, par (2), (13) et (24)

$$F_{\mathcal{A}(U)\cup\{L\}}(z) = \frac{F_{\mathcal{A}(U)}(z)}{1-z^L} \equiv \frac{U(z)}{1-z^L} \equiv F_{\mathcal{A}(P/Q)}(z) \pmod 2$$

et, par la propriété caractéristique (13), $\mathcal{A}(P/Q) = \mathcal{A}(U) \cup \{L\}$. De même, si $2^h L \notin \mathcal{A}(U)$ et $\{L, 2L, \dots, 2^{h-1}L\} \subset \mathcal{A}(U)$, on pose $\mathcal{A}' = \mathcal{A}(U) \backslash \{L, 2L, \dots, 2^{h-1}L\} \cup \{2^h L\}$, et l'on a par (2), (13) et (24)

$$\begin{aligned} F_{\mathcal{A}'}(z) &= F_{\mathcal{A}(U)}(z) \frac{(1-z^L)(1-z^{2L})\cdots(1-z^{2^{h-1}L})}{(1-z^{2^h L})} \\ &\equiv F_{\mathcal{A}(U)}(z) \frac{(1+z^L)(1+z^{2L})\cdots(1+z^{2^{h-1}L})}{(1-z^{2^h L})} = \frac{F_{\mathcal{A}(U)}(z)}{(1-z^L)} \\ &\equiv \frac{P(z)}{Q(z)} \pmod 2 \end{aligned}$$

ce qui, par la propriété caractéristique (13), implique $\mathcal{A}(P/Q) = \mathcal{A}'$.
- 2ème cas. Si pour tout $h \geq 0$, $2^h L \in \mathcal{A}(U)$, on pose $\mathcal{A}' = \mathcal{A}(U) \backslash \{L, 2L, \dots, 2^h L, \dots\}$ et l'on a

$$F_{\mathcal{A}'}(z) = F_{\mathcal{A}(U)}(z)(1-z^L)(1-z^{2L})\cdots(1-z^{2^h L})\cdots.$$

En utilisant l'identité

$$\prod_{h=0}^{\infty}(1+X^{2^h}) = \frac{1}{1-X}, \tag{25}$$

par (13) et (24) il vient $F_{\mathcal{A}'}(z) \equiv U(z)/(1-z^L) \pmod 2$ et l'on conclut, comme dans le premier cas, $\mathcal{A}(P/Q) = \mathcal{A}'$ par (13).

Remarque. A l'aide de Maple, pour chacun des 10 795 couples (P, Q) de polynômes de degré inférieur ou égal à 7, satisfaisant (19) et $Q \neq 1$, nous avons calculé l'ordre L de Q, le polynôme U défini par (24) et h qui est le plus petit entier tel que $2^h L$ n'appartienne pas à $\mathcal{A}(U)$; si, pour tout $j \geq 0$, $2^j L \in \mathcal{A}(U)$, on pose $h = \infty$. La distribution des 10 795 valeurs de h est donnée dans le tableau ci-dessous:

$h =$	0	1	2	3	4	5	6	7	8	9	10	∞
	5578	2619	1296	505	474	137	29	19	19	3	3	113

Explicitons le cas $P := 1 + X + X^2 + X^4 + X^6$, $Q = 1 + X^3 + X^4 + X^5$. On a $L = 14$, $U = (1 + X^7)/(1 + X)V$ avec $V = 1 + X^6 + X^9 = T(X^3)$. Comme V est un polynôme en X^3, $\mathcal{A}(V) = 3\mathcal{A}(T)$ ne contient que des multiples de 3. Posons

$$\mathcal{A}' = \mathcal{A}(V) \cup \{1, 7, 14, 28, \dots, 2^j \cdot 7, \dots\}.$$

On a, par (2), (13) et (25)

$$F_{\mathcal{A}'}(X) = F_{\mathcal{A}(V)}(X)\frac{1}{1-X}\prod_{j=1}^{\infty}\frac{1}{1-X^{2^j 7}} \equiv \frac{1+X^7}{1+X}V \equiv U \pmod 2.$$

Par l'unicité de l'ensemble $\mathcal{A}(U)$, il s'ensuit que $\mathcal{A}' = \mathcal{A}(U)$; ainsi $\mathcal{A}(U)$ contient $2^j L = 14 \cdot 2^j$ pour tout $j \geq 0$ et donc $h = \infty$.

Proposition 2.2. *Soient $A_{P,Q}(x)$ (resp. $A_U(x)$) les fonctions de compte associées à $\mathcal{A}(P/Q)$ (resp. à $\mathcal{A}(U)$) définies par (1), alors, lorsque $x \to \infty$, on a $A_{P,Q}(x) = A_U(x) + O(\log x)$.*

Démonstration. Appliquons le Théorème 2.1. Dans le premier cas, $\mathcal{A}(P/Q)$ et $\mathcal{A}(U)$ diffèrent par un nombre fini de points et, pour $x > 2^h L$, on a $A_{P,Q}(x) = A_U(x) - h + 1 = A_U(x) + O(1)$.

Dans le deuxième cas, on a $\mathcal{A}(P/Q) = \mathcal{A}(U) \backslash G$ avec $G = \{2^i L, i \geq 0\}$ et $A_{P,Q}(x) = A_U(x) - G(x)$ avec

$$0 \leq G(x) = \sum_{0 \leq i \leq \frac{\log(x/L)}{\log 2}} 1 = 1 + \lfloor (\log(x/L))/\log 2 \rfloor = O(\log x)$$

ainsi notre résultat est établi.

3. La périodicité de $(\sigma(\mathcal{A}(P/Q), 2^k n) \bmod 2^{k+1})_{n \geq 1}$

Pour $n \geq 1$, en désignant par $\sigma(\mathcal{A}(P/Q), n)$ la fonction définie par (4), on a le résultat suivant

Théorème 3.1. *Soient $P, Q \in \mathbb{F}_2[z]$ satisfaisant (19), et $\mathcal{A}(P/Q) \subset \mathbb{N}$ défini par (20), alors pour tout $k \geq 0$, la suite $(\sigma(\mathcal{A}(P/Q), 2^k n) \bmod 2^{k+1})_{n \geq 1}$ est périodique. Si l'on note par q_k la plus petite des périodes, alors on a*

$$q_k \text{ est impair,} \tag{26}$$

$$q_k \text{ divise } q_{k+1} \tag{27}$$

et pour tout $k \geq k_0$, on a

$$q_k = q \text{(fixè)}. \tag{28}$$

Remarque. Lorsque $Q = 1$, ce théorème est démontré dans [1] (voir (17) et (18)). La démonstration de [1] peut s'étendre au cas $Q \neq 1$ (cf. [5], Chapter 1). Nous donnons ci-dessous une preuve du Théorème 3.1 basée sur le Théorème 2.1.

Démonstration. D'après le Théorème 2.1, il existe un polynôme $U \in \mathbb{F}_2[z]$ et $\mathcal{A}(U) \subset \mathbb{N}$, tel que la fonction génératrice $F_{\mathcal{A}(P/Q)}$ vérifie (24). On écrit $L = 2^\alpha \beta$, avec $\alpha \geq 0$ et β impair. On note, pour $j \geq 0$ et $k \geq 0$

$$\begin{aligned} S_j(n,k) &= \sigma(\{2^j L\}, 2^k n) \bmod 2^{k+1} \\ &= \begin{cases} 0 & \text{si } \alpha + j \geq k+1 \text{ ou } \beta \nmid n \\ 2^j L \bmod 2^{k+1} & \text{si } \alpha + j \leq k \text{ et } \beta \mid n. \end{cases} \end{aligned} \tag{29}$$

En effet,

$$(2^j L = 2^{\alpha+j}\beta \text{ divise } 2^k n) \qquad \text{et} \qquad (\alpha + j \leq k) \Longrightarrow \beta \mid n,$$

et (4) implique (29). Pour j et k fixés, la suite $(S_j(n,k))_{n\geq 1}$ est donc périodique, et β est une période. Maintenant, le Théorème 2.1 dit qu'il existe dans tous les cas deux sous-ensembles $\mathcal{J}^+$ et $\mathcal{J}^-$ de $\{0,1,2,\ldots\}$, éventuellement vides, tels que, en posant $\mathcal{E}^+ = \{2^j L, j \in \mathcal{J}^+\}$, $\mathcal{E}^- = \{2^j L, j \in \mathcal{J}^-\}$, on ait

$$\mathcal{A}(P/Q) = \mathcal{A}(U) \cup \mathcal{E}^+ \backslash \mathcal{E}^-, \qquad \mathcal{E}^- \subset \mathcal{A}(U), \qquad \mathcal{E}^+ \cap \mathcal{A}(U) = \emptyset.$$

Il s'ensuit que, pour k fixé, et $n \geq 1$,

$$\sigma(\mathcal{A}(P/Q), n2^k) \equiv \sigma(\mathcal{A}(U), n2^k) + \sum_{\substack{j\in\mathcal{J}^+\\ j\leq k-\alpha}} S_j(n,k) - \sum_{\substack{j\in\mathcal{J}^-\\ j\leq k-\alpha}} S_j(n,k) \pmod{2^{k+1}}. \tag{30}$$

Mais, par (17), $(\sigma(\mathcal{A}(U), n2^k) \bmod 2^{k+1})_{n\geq 1}$ est périodique de période, disons, T_k, et chaque $S_j(n,k)$ appairaissant dans (30) est, modulo 2^{k+1}, par (29), périodique en n, de période β. Il suit donc de (30) que $(\sigma(\mathcal{A}(P/Q), n2^k) \bmod 2^{k+1})_{n\geq 1}$ est périodique, et que sa plus petite période q_k vérifie

$$q_k \text{ divise } \operatorname{ppcm}(T_k, \beta). \tag{31}$$

Comme T_k et β sont impairs, (26) découle de (31). La démonstration de (27) se fait de la même manière que (3)–(9) dans [1]: un diviseur de $2^{k+1}n$ est soit un diviseur de $2^k n$ soit un multiple de 2^{k+1}. Il s'ensuit que, avec $\mathcal{A} = \mathcal{A}(P/Q)$

$$\sigma(\mathcal{A}, 2^{k+1}n) \equiv \sigma(\mathcal{A}, 2^k n) \pmod{2^{k+1}} \tag{32}$$

et, en substituant $n + q_{k+1}$ à n,

$$\sigma(\mathcal{A}, 2^{k+1}(n+q_{k+1})) \equiv \sigma(\mathcal{A}, 2^k(n+q_{k+1})) \pmod{2^{k+1}}. \tag{33}$$

Comme $\sigma(\mathcal{A}, 2^{k+1}n) \equiv \sigma(\mathcal{A}, 2^{k+1}(n+q_{k+1})) \pmod{2^{k+1}}$ (car q_{k+1} est une période de $\sigma(\mathcal{A}, 2^{k+1}n) \bmod 2^{k+2}$ donc aussi de $\sigma(\mathcal{A}, 2^{k+1}n) \bmod 2^{k+1}$), on déduit de (32) et (33) que

$$\sigma(\mathcal{A}, 2^k(n+q_{k+1})) \equiv \sigma(\mathcal{A}, 2^{k+1}n) \equiv \sigma(\mathcal{A}, 2^k n) \pmod{2^{k+1}}$$

autrement dit, q_{k+1} est une période de la suite $(\sigma(\mathcal{A}, n2^k) \bmod 2^{k+1})_{n\geq 1}$; or, la période minimale de cette suite est par définition q_k, ce qui prouve (27).

Pour démontrer (28), on a d'après (18), $T_k = T$ *fixé* pour tout $k > k_0$. Pour la relation de divisibilité, par (27), la suite q_k est croissante et est majorée par ppcm (T, β), ce qui démontre (28).

Références

[1] F. Ben Saïd, J.-L. Nicolas, Sets of parts such that the partition function is even, Acta Arithmetica 106 (2003) 183–196.

[2] F. Ben Saïd, J.-L. Nicolas, Even partition functions, Séminaire Lotharingien de Combinatoire 46 (2002) B 46i. Available from http://www.mat.univie.ac.at/~slc.

[3] F. Ben Saïd, On a conjecture of Nicolas–Sárközy about partitions, Journal of Number Theory 95 (2002) 209–226.
[4] F. Ben Saïd, On some sets with even valued partition function, à paraître, The Ramanujan Journal (2004).
[5] H. Lahouar, Thèse de I'Université de Tunis, à paraître (2004).
[6] J.-L. Nicolas, I.Z. Ruzsa, A. Sárközy, On the parity of additive representation function, Journal of Number Theory 73 (1998) 292–317.
[7] J.-L. Nicolas, A. Sárközy, On the parity of generalized partition functions, in: M.A. Bennett, B.C. Berndt, N. Boston, H.G. Diamond, A.J. Hildebrand, W. Philip (Eds.), Number Theory for the Millennium, vol. III, A.K. Peters, 2002, pp. 55–72.
[8] J.-L. Nicolas, On the parity of generalized partition functions II, Periodica Mathematica Hungarica 43 (2001) 177–189.
[9] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Application, Cambridge University Press, 1994.